(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 407 553 A1

(12) **EUROPEAN PATENT APPLICATION**
published in accordance with Art. 153(4) EPC

(43) Date of publication:
28.11.2018 Bulletin 2018/48

(21) Application number: **17849864.8**

(22) Date of filing: **12.04.2017**

(51) Int Cl.:
H04L 12/741 *(2013.01)*

(86) International application number:
PCT/CN2017/080245

(87) International publication number:
WO 2018/176510 (04.10.2018 Gazette 2018/40)

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
MA MD

(30) Priority: **30.03.2017 CN 201710203829**

(71) Applicant: **Wangsu Science & Technology Co., Ltd.**
Shanghai 200030 (CN)

(72) Inventors:
- **XU, Jiaxuan**
  Shanghai 200030 (CN)
- **CHENG, Duyong**
  Shanghai 200030 (CN)
- **WU, Shengwan**
  Shanghai 200030 (CN)

(74) Representative: **Hanna Moore + Curley**
Garryard House
25/26 Earlsfort Terrace
Dublin 2, D02 PX51 (IE)

(54) PPPOE MESSAGE TRANSMISSION METHOD AND PPPOE SERVER

(57) The present disclosure provides a PPPoE packets transmitting method and a PPPoE server. The method comprises: registering, by a PPPoE server, a PPPoE protocol packet sniffer with a Linux kernel and an Internet Protocol Version 4 (IPV4) protocol packet sniffer with a Netfilter framework, and adding a user's IP address and MAC address to authenticated user information, receiving, by the PPPoE server, a packet, and calling, by the PPPoE server, the PPPoE protocol packet sniffer or the IPV4 protocol packet sniffer to process and transmit the packet according to the authenticated user information. In the present disclosure, during a user's dial-up logon or logoff, the creation and deletion of a network interface are not required, which can improve the logon and logoff speeds.

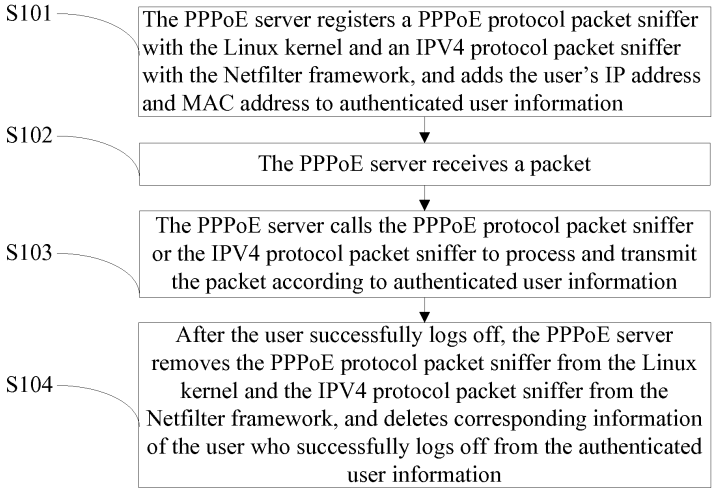

FIG. 1

EP 3 407 553 A1

Description

FIELD OF THE DISCLOSURE

[0001] The present disclosure generally relates to network transmission technology and, more particularly, to a method for transmitting PPPoE packets and a PPPoE server thereof.

BACKGROUND

[0002] With the development of network technology, the broadband access has currently become a major way of useraccess.The major way of the broadband dial-up and authentication is the Point-to-Point Protocol over Ethernet (PPPoE.) The performance indicators of a PPPoE Broadband Remote Access Server generally include the logon and logoff speedsof the dial-up and authentication.

[0003] The existing solution for implementing a PPPoE Broadband Remote Access Server on the Linux platform is to create a virtual network interface (e.g., ppp0) for each dial-up user and delete the virtual network interface when the user logs off. The objectives of creating the virtual network interface is to realize the termination of PPPoE packets and the forwarding of data packets. However, the creation and deletion of a virtual network interface involves a lot of time-consuming tasksin the bottom layer, for example, memory request and release, system call, central processing unit (CPU) privilege level switch. The creation and deletion of the above virtual network interface can lead to a slow dial-up logon and logoff.

SUMMARY

[0004] To solve the problem of the existing broadband access technologies, in which the creation and deletion of a virtual network interface can lead to a slow dial-up logon and logoff.The present disclosure provides a PPPoE packets transmitting method and a PPPoE server. The technical solutions are as follows.

[0005] One aspect of the present disclosure provides a method for PPPoE packets transmitting comprising: registering, by a PPPoE server, a PPPoE protocol packet sniffer with a Linux kernel and an Internet Protocol Version 4 (IPV4) protocol packet sniffer with a Netfilter framework, and adding a user's Internet Protocol (IP) address and media access control (MAC) address to authenticated user information, receiving, by the PPPoE server, a packet; and calling, by the PPPoE server, the PPPoE protocol packet sniffer or the IPV4 protocol packet sniffer to process and transmit the packet according to the authenticated user information.

[0006] Furthermore, calling, by the PPPoE server, the PPPoE protocol packet sniffer or the IPV4 protocol packet sniffer to process and transmit the packet according to the authenticated user information, includes:determining, by the PPPoE server, whether the packet is a user's uplink packet or a user's downlink packet, when the packet is the user's uplink packet, calling, by the PPPoE server, the PPPoE protocol packet sniffer, and determining, by the PPPoE protocol packet sniffer, whether the packet is a PPPoE data packet and, when the packet is the PPPoE data packet, according to the authenticated user information, striping off header information of the PPPoE data packet, and forwarding the processed PPPoE data packet to the Internet-side, and when the packet is the user's downlink packet, calling, by the PPPoE server, the IPV4 protocol packet sniffer, and adding, by the IPV4 protocol packet sniffer, according to the authenticated user information, header information to the user's downlink packet and forwarding the processed PPPoE data packet to the user.

[0007] Furthermore, calling, by the PPPoE server, the PPPoE protocol packet sniffer, and determining, by the PPPoE protocol packet sniffer, whether the packet is the PPPoE data packet and, when the packet is the PPPoE data packet, according to the authenticated user information, striping off the header information of the PPPoE data packet, and forwarding the processed PPPoE data packet to the Internet-side, includes: determining, by the PPPoE protocol packet sniffer, according to a value of an Ethernet packet protocol field, that the PPPoE is currently in a PPP Session Stage, determining, by the PPPoE protocol packet sniffer, according to a PPP packet header protocol field, that the packet is the PPPoE data packet, obtaining, by the PPPoE protocol packet sniffer, the MAC address from an Ethernet packet header and the IP address from an IPV4 packet header, comparing, by the PPPoE protocol packet sniffer, the MAC address and IP address with information in the authenticated user information, when the MAC address and IP address match with information in the authenticated user information, determining that the user belongs to authenticated users and striping off the header of the PPPoE data packet to forward the processed PPPoE data packet to the Internet-side, and when the MAC address and IP address do not match with information in the authenticated user information, determining that the user does not belong to the authenticated users and throwing away the PPPoE data packet.

[0008] Furthermore, calling, by the PPPoE server, the IPV4 protocol packet sniffer, and adding, by the IPV4 protocol packet sniffer, according to the authenticated user information, header information to the user's downlink packet and forwarding the processed PPPoE data packet to the user, includes: obtaining, by the IPV4 protocol packet sniffer, the user's IP address from the IPV4 packet header, comparing, by the IPV4 protocol packet sniffer, the IP address with the information in the authenticated user information, when the IP address matches with the information in the authenticated user information, determining that the user belongs to the authenticated users and adds the header information to the user's downlink packet to forward the processed packet to the user, and when the IP address does not match with the

information in the authenticated user information, determining that the user does not belong to the authenticated users and throwing away the downlink packet.

[0009] Furthermore, every time the user logs on the Internet, the PPPoE protocol packet sniffer registers with the Linux kernel and the IPV4 protocol packet sniffer registers with the Netfilter framework by the PPPoE server, and every time after the user successfully logs off, the PPPoE server removes the PPPoE protocol packet sniffer from the Linux kernel and the IPV4 protocol packet sniffer from the Netfilter framework, and deletes corresponding information of the user who successfully logs off from the authenticated user information.

[0010] Furthermore, when the user logs on the Internet for a first time after user initialization or restart,the PPPoE protocol packet sniffer registers with the Linux kernel and the IPV4 protocol packet sniffer registers with the Netfilter framework, and after the user successfully logs off, deletes the user's corresponding information from the authenticated user information

[0011] Furthermore, the PPPoE server registers the IPV4 protocol packet sniffer with a POSTROUTING chain of the Netfilter framework.

[0012] Another aspect of the present disclosure provides an Point-to-Point Protocol over Ethernet (PPPoE) server comprising:a registration unit configured to register a PPPoE protocol packet sniffer with a Linux kernel and an IPV4 protocol packet sniffer with a Netfilter framework, and add a user's IP address and MAC address to authenticated user information, a receiving unit configured to receive a packet, anda processing unit configured to call the PPPoE protocol packet sniffer or the IPV4 protocol packet sniffer and, according to the authenticated user information, process and transmit the packet.

[0013] Furthermore, a determination module is configured to determine whether the packet is a user's uplink packet or a user's downlink packet.

[0014] A first call module is configured, when the packet is the user's uplink packet, to call the PPPoE protocol packet sniffer, the PPPoE protocol packet sniffer determines whether the packet is a PPPoE data packet and, when the received packet is the PPPoE data packet, according to the authenticated user information, strips off-header information of the PPPoE data packet, and forwards the processed PPPoE data packet to the Internet-side.

[0015] A second call module is configured, when the packet is the user's downlink packet, to call the IPV4 protocol packet sniffer, the IPV4 protocol packet sniffer, according to the authenticated user information, adds header information to the user's downlink packet and forwards the processed PPPoE data packet to the user.

[0016] Furthermore, the PPPoE protocol packet sniffer includes:

A first determination module is configured, according to a value of an Ethernet packet protocol field, to determine that the PPPoE is currently in a PPP Session Stage;

A second determination module is configured, according to a PPP packet header protocol field, to determine that the packet is the PPPoE data packet;

A first acquisition module is configured to obtain the MAC address from an Ethernet packet header and the IP address from an IPV4 packet header;

A first comparison module is configured to compare the MAC address and IP address with information in the authenticated user information;

A first forwarding module is configured, when the MAC address and IP address match with information in the authenticated user information, to determine that the user belongs to authenticated users andstrip off header of the PPPoE data packet to forward the processed PPPoE data packet to the Internet-side; and

A first throw-away module is configured, when the MAC address and IP address do not match with information in the authenticated user information, to determine that the user does not belong to the authenticated users and throw away the PPPoE data packet.

[0017] Furthermore, the IPV4 protocol packet sniffer includes: a second acquisition module configured to obtain the user's IP address from the IPV4 packet header, a second comparison module configured to compare the IP address with the information in the authenticated user information, a second forwarding module configured, when the IP address matches with information in the authenticated user information, to determine that the user belongs to the authenticated users and add the header information to the user's downlink packet to forward the processed packet to the user, and a second throw-away-module configured, when the IP address does not match with information in the authenticated user information, to determine that the user does not belong to the authenticated users and throw away the downlink packet.

[0018] Furthermore, the PPPoE server also includes a removing unit configured, after the user successfully logs off, to remove the PPPoE protocol packet sniffer from the Linux kernel and the IPV4 protocol packet sniffer from the Netfilter framework, and to delete the user's corresponding information from the authenticated user information.

[0019] The beneficial effect of the technical solutions according to embodiments of the present disclosure is as the following. The registration and deletion of a IPV4protocol packet sniffer in the Netfilter framework and a PPPoE protocol packet sniffer in the Linux kernel are used to replace the creation and deletion of a virtual network interface , and the authenticated user information

is stored. After receiving the packet, the PPPoE server calls the corresponding protocol packet sniffer and according to the authenticated user information to process the packet header and transmit the processed packet. As such, the correct processing and the normal transmission of the user's uplink data packets and downlink data packets can be ensured. The proposed method reduces the time cost for the creation of the network interface during the logon process and the time cost for the destruction of the network interface during the logoff process, such that the logon and logoff speeds for user dial-up during the process of a PPPoE broadband access on the Linux platform can be effectively increased.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] In order to provide a clearer illustration of technical solutions of the present disclosure, the drawings used in the description of the disclosed embodiments are briefly described below. It is apparent that the following drawings are merely some of embodiments of the present disclosure. Other drawings may be obtained based on the disclosed drawings by those skilled in the art without creative efforts.

FIG. 1 is a flow chart of a method for transmitting PPPoE packets according to embodiments of the present disclosure;

FIG. 2 isflow chart ofprocessing of a user's uplink data packet according to embodiments of the present disclosure;

FIG. 3 isflow chart ofprocessing ofa user's downlink data packet according to embodiments of the present disclosure; and

FIG. 4 is a block diagram of a PPPoE server according to embodiments of the present disclosure.

DETAILED DESCRIPTION

[0021] In order to make the objectives, technical solutions, and advantages of the present disclosure clearer, embodiments of the present disclosure are described in detail below with reference to the drawings.

[0022] To solve the problem of the existing broadband access technology in which the creation and deletion of the virtual network interface can lead toa slow dial-up logon and logoff, the virtual network interface can be replaced to increase the logon and logoff speeds. However, the following problems caused by the absence of the virtual network interface need to be considered for solving.

(1)After receiving the user'suplink data packets and downlink data packets, the PPPoE server cannot process the uplink data packets and downlink data packets, which includesadding and deleting the PPPoE packet header.

(2)The kernel forwards data according to the network interface and the routing table. There is no network interface that is created corresponding to the client-side, thus, the user'suplink data packets and downlink data packets cannot be normally forwarded.

[0023] In view of the above problems, embodiments of the present disclosure provide a method for transmitting PPPoE packets. As shown in FIG. 1, the method includes the following steps S101 to S104.

[0024] At step S101, the PPPoE server registers a PPPoE protocol packet sniffer with the Linux kernel and an Internet Protocol Version 4 (IPV4) protocol packetsniffer with the Netfilter framework, and adds the user's Internet Protocol(IP) address and media access control(MAC) address to authenticated user information.

[0025] In the present embodiment, after the user dial-up authorization succeeds, the PPPoE server starts to register the PPPoE protocol packet sniffer and the IPV4 protocol packet sniffer. The user dial-up authentication refers to the process that the userenters the user name and password for dial-up Internet connectionon the client-side, and the server-sidedetermines whether the received user name and password are correct. If correct, a message is returned to the client-side and the dial-up authentication succeeds. Specifically, the PPPoE server registers the PPPoE protocol packet sniffer with the Linux kernel and the IPV4 protocol packet sniffer with the POSTROUTING chain of the Netfilter framework. The PPPoE protocol packet sniffer is mainly used for terminating the user's uplink PPPoE packet, and the IPV4 protocol packet snifferis mainly used to add thePPPoE packet header to the user's downlink data packet.The authenticated user information can be stored in the form of a list, which is easy for query and comparison.

[0026] In the present embodiment,the PPPoE protocol packet sniffer and the IPV4 protocol packet sniffer may be registeredevery time that the user logs on the Internet. The PPPoE protocol packet sniffer and the IPV4 protocol packet sniffer may also be registered, when the user logs on the Internet for a first time after user initialization or restart. The present disclosure is not limited thereto.

[0027] At step S102, the PPPoE server receives a packet. The PPPoE data packet belongs to the Layer 2 packet and is carried in the data field of the Ethernet packet for transmission.The value of the Ethernet packet's protocol field is 0x8863, which indicates that the PPPoE is in the Activity Discovery Phase. The value of the Ethernet packet's protocol field is 0x8864, which indicates that the PPPoE is in the PPP Session Stage. The Layer 3 packet corresponding to the PPPoE data packet are the IPV4 packet. The PPPoE data packet carries the Point-to-Point Protocol (PPP) packet. The PPP packet-header protocol field is used to distinguish the contents of the data packets carried by the PPPoE packets. For example, 0021 represents the IP protocol, and C021 rep-

resents the Link Control Protocol (LCP).

[0028] At step S103, the PPPoE server calls the PPPoE protocol packet sniffer or the IPV4 protocol packet sniffer to process and transmit the packet according to the authenticated user information.

[0029] At step S104, after the user successfully logs off, the PPPoE server removes the PPPoE protocol packet sniffer from the Linux kernel and the IPV4 protocol packet sniffer from the Netfilter framework, and deletes corresponding information of the user who successfully logs offfrom the authenticated user information.

[0030] Step 104 is not a necessary step, which corresponds to the situationwhen the PPPoE protocol packet sniffer and the IPV4 protocol packet sniffer are registered every time that the user logs on the Internet. That is, if the PPPoE server removes the PPPoE protocol packet sniffer from the Linux kernel and the IPV4 protocol packet sniffer from the Netfilter framework, and deletes the user's corresponding information from the authenticated user information, then the PPPoE protocol packet sniffer and the IPV4 protocol packet sniffer need to be registered every time that the user logs on the Internet.

[0031] In other embodiments, the PPPoE protocol packet sniffer and the IPV4 protocol packet sniffer may also be registered,when the user logs on the Internet for a first time after user initialization or restart.After the user successfully logs off, only the user's corresponding information is deleted from the authenticated user information, and step 104 is not necessary. Therefore, the user's logon time can be further shorten.

[0032] In the above-described embodiment,the registration and deletion of a IPV4protocol packet sniffer in the Netfilter framework and a PPPoE protocol packet sniffer in the Linux kernel are used to replace the creation and deletion of a virtual network interface,and the authenticated user information is stored. After receiving the packet, the PPPoE server calls the corresponding protocol packet sniffer and according to the authenticated user information to process the packet header and transmit the processed packet. As such, the correct processing and the normal transmission of the user's uplink data packets and downlink data packets can be ensured. The proposed method reduces the time cost for the creation of the network interface during the logon process and the time cost for the destruction of the network interface during the logoff process, such that the logon and logoff speeds for user dial-up during the process of a PPPoE broadband access on the Linux platform can be effectively increased.

[0033] In an embodiment, step S103 includes the followings. The PPPoE server determines whether the received packet is the user's uplink packet or the user's downlinkpacket. If the received packet is the user'suplink packet, the PPPoE server calls the PPPoE protocol packet sniffer. The PPPoE protocol packet sniffer determines whether the received packet is a PPPoE data packet and, if the received packet is a PPPoE data packet, according to the authenticated user information, strips off header information of the PPPoE data packet, and forwards the processed PPPoE data packet to the Internet-side. If the received packet is the user's downlink packet, the PPPoE server calls the IPV4 protocol packet sniffer. The IPV4 protocol packet sniffer, according to the authenticated user information, adds header information to the user's downlink packet and forwards the processed PPPoE data packet to the user. The Internet-side is relative to the client-side. After obtaining dial-up Internet access, the user may send data to the Internet-side or receive data from the Internet-side.

[0034] In the above embodiment, for the user's uplink data packets and downlink data packets, the sniffers used are different and the processing of the header information is also different. Therefore, the packet needs to be determined to further determine the subsequent processing procedure and realize the normal forwarding of the user's uplink data packets and downlink data packets. At the same time, it is also necessary to determine, according to the authenticated user information stored in advance,whether the current user has authenticated. If the user is not authenticated, the unnecessary packet isdirectly thrown awayto avoid the occupation of resources. If the user is authenticated, the packet is forwarded to the corresponding user or the Internet-side to ensure the smooth transmission of the packet.

[0035] Specifically, for the user's uplink data packet, after thePPPoE server calls the PPPoE protocol packet sniffer, the PPPoE protocol packet sniffer performs the following operations. The PPPoE protocol packet sniffer, according to the value of the Ethernet packet protocol field, determines that the PPPoE is currently in the PPP Session Stage(as described above, the value of the protocol fieldis 0x8864 indicating that the PPPoE is in the PPP Session Stage.) The PPPoE protocol packet sniffer, according to the PPP packet header protocol field, determines that the packet is a PPPoE packet (as described above, the PPP packet header protocol field is 0021 indicating the IP protocol, and the corresponding Layer 2 packet is a PPPoE packet.) The PPPoE protocol packet sniffer obtains the MAC address from the Ethernet packet header and the IP address from the IPV4 packet header. The PPPoE protocol packet sniffer compares the MAC address and IP address with information in the authenticated user information and, if match, determines that the user belongs to the authenticated users and strips off header of the PPPoE data packet to forward the processed PPPoE data packet to the Internet-side and, if not match, determines that the user does not belong to the authenticated users and throws away the PPPoE data packet. If the intercepted packet is not a PPPoE data packet, the processing of the PPPoE control packet is entered, and the control packet processing method will not be discussed in the present disclosure.

[0036] Specifically, for the user's downlink packet, after the PPPoE server calls the IPV4 protocol packet sniffer, the IPV4 protocol packet sniffer performs the following operations. The IPV4 protocol packet sniffer ob-

tains the user's IP address from the IPV4 packet header. The IPV4 protocol packet sniffercompares the IP address with information in the authenticated user information and, if match, determines that the user belongs to the authenticated users and adds the header information to the user's downlink packetto forward the processed packet to the user and, if not match, determines that the user does not belong to the authenticated users and throws away the downlink packet.

[0037] The processingprocedureof the user's uplink and downlink data according to embodiments of the present disclosure will be described below with reference to FIGs. 2 and 3.

[0038] FIG. 2 is flow chart of processing of the user's uplink data packet according to embodiments of the present disclosure. As shown in FIG.2, the processing procedure of the user's uplink data packetincludes the following steps.

[0039] At step S201, a network card arranged at the client-side receives a packet.

[0040] At step S202,the PPPoE server calls the PPPoE protocol packet sniffer to determine whether the received packet is a PPPoE data packet and, if yes, the process proceeds to step S203 and, if no, the process proceeds to step S206.

[0041] At step S203,according to anauthorized user-information list, whether the user has been authorized is determined and, if yes, the process proceeds to step S204 and, if no, the packet is directly thrown away, and the process proceeds to step S213.

[0042] At step S204,the PPPoE protocol packet sniffer strips off the headerof the PPPoE data packet.

[0043] At step S205,the PPPoE protocol packet sniffer forwards the processed PPPoE data packet to the Internet-side, and the process proceeds to step S213.

[0044] At step S206,the PPPoE server determines whether the user dial-up authentication is successful and, if yes, the process proceeds to step S207 and, if not, the process proceeds to step S209.

[0045] At step S207,the PPPoE server registers the PPPoE protocol packet sniffer with the Linux kernel and the IPV4 protocol packet sniffer with the Netfilter framework.

[0046] At step S208,the PPPoE server adds user information (IP address and MAC address) to the authorized user information list, and then proceeds to step S213.

[0047] At step S209, the PPPoE server determines whether the user logs off successfully and, if yes, the process proceeds to step S210; if not, the process proceeds to step S212.

[0048] At step S210, the PPPoE server removes the PPPoE protocol packet sniffer from the Linux kernel and the IPV4 protocol packet sniffer from the Netfilter framework.

[0049] At step S211, the PPPoE server deletes information corresponding to the user from the authorized user information list, and thenthe process proceeds to step S213.

[0050] At step S212, the other processing of PPPoE control packet is performed and then the process proceeds to step S213.

[0051] Step S213, the process completes.

[0052] FIG. 3 is flow chart of processing of the user's downlink data packet according to embodiments of the present disclosure. As shown in FIG. 3, the processing procedure of the user's downlink data packet includes the following steps.

[0053] At step S301, a network card arranged at the Internet-side receives a packet.

[0054] At step S302, the PPPoE server calls the IPV4 protocol packet sniffer and the IPV4 protocol packet sniffer receives the packet.

[0055] At step S303, the IPV4 protocol packet sniffer determines whether the target user is anauthorized user and, if yes, the process proceeds to step S304 and, if not, the packet is directly thrown away and the process proceeds to step S306.

[0056] At step S304, the IPV4 protocol packet sniffer adds the header of the PPPoE data packet to the packet.

[0057] At step S305, the IPV4 protocol packet sniffer performs the forwarding and forwards the packet to the network card arranged at the client-side.

[0058] Step S306, the process completes.

[0059] The PPPoE protocol includes the Activity Discovery Phase and the PPP Session Stage.When a client-host wants to start a PPP Session, an Activity Discovery Phase needs to be firstly implemented to identify the MAC address of the opposite party and establish a unique PPP Session ID (identification) .During the Activity Discovery Phase, the client-host discovers all the servers and chooses one of them to establish a point-to-point connection. When a PPP Session is established, the entire Activity Discovery Phase is completed and the PPP Session Stageis entered. In the PPP Session Stage, between the host and the server, according to the PPP protocol, PPP data is transmitted, and various PPP negotiations and the PPP data transmission are performed. The transmitted packet contains the PPP Session ID determined at the Activity Discovery Phase and the PPP Session ID remains unchanged.

[0060] The user first goes through the Activity Discovery Phase and, after the completion of the Activity Discovery Phase, enters thePPP Session Stage.After the user authentication succeeds, the PPPoE server does not create the virtual network interface corresponding to the user, but registers the PPPoE protocol packet sniffer with the Linux kernel and the IPV4 protocol packet sniffer with the Netfilter framework, and adds the user IP and the MAC mapping the authorized user information list.

[0061] The PPPoE protocol packet sniffer is called when the user's uplink packet passes through the PPPoE server. The PPPoE protocol packet sniffer, according to the contents of the authorized user information list, determines whether the user who sent the packet has successfully authenticated.If the user's uplink packet is the

authenticateduser's uplink packet, the PPPoE packet sniffer strips off the PPPoE packet header and performs the forwarding to forward the packet to the network card arranged at the Internet-side. As such, the problem of normal forwarding of the user's uplink data packet is solved.

[0062] The PPPoE protocol packet sniffer obtains the value of the Ethernet protocol field firstly and, if the PPPoE is in the PPP Session Stage (0x8864), obtains the PPP packet header protocol field and, if the value is 0021, the packet type is considered as a PPPoE data packet. The PPPoE protocol packet sniffer obtains the MAC address from the Ethernet packet header and the IP address from the IPV4 packet header, and compares the MAC address and the IP address with the entries in the authentication address table and, if match, forwards the packet to the Internet-side, otherwise, throws away the packet.If the packet type is not a PPPoE data packet, the other processing of the PPPoE control packet is performed.

[0063] The IPV4 protocol packet sniffer is called when the user's downlink packet passes through the PPPoE server. The IPV4 protocol packet sniffer, according to the contents of the authorized user information list, determines whether the target user of the packet has successfully authenticated. If the target user is an authenticated user, the IPV4 protocol packet snifferadds the PPPoE packet header and performs the forwarding to forward the packet to the network card arranged at the client-side. As such, the problem of normal forwarding of the user's downlink data packet is solved.

[0064] The embodiments of the present disclosure also provide a PPPoE server, which can be used to implement the above-described method for transmitting PPPoE packets. The specific implementation thereof may refer to the above-described method according to embodiment of the present disclosure. As shown in FIG. 4, the PPPoE server includes a registration unit 41, a receiving unit 42, a processing unit 43, and a removing unit 44. The function of each unit is described in detail below.

[0065] The registration unit 41 is configured, after the user dial-up authorization succeeds,to register a PPPoE protocol packet sniffer with the Linux kernel and an IPV4 protocol packet sniffer with the Netfilter framework, and add the user's IP address and MAC address to authenticated user information.

[0066] The receiving unit 42 is communicated with the registration unit 41 and is configured to receive a packet.

[0067] The processing unit 43is communicated with the receiving unit 42and is configured to call the PPPoE protocol packet sniffer or the IPV4 protocol packet sniffer and, according to the authenticated user information, process and transmit the received packet.

[0068] The removing unit 44 communicated with the processing unit 43 is configured,after the user successfully logs off, to remove the PPPoE protocol packet sniffer from the Linux kernel and the IPV4 protocol packet sniffer from the Netfilter framework, and delete user's corresponding information from the authenticated user information. The removing unit 44is not a necessary unit, which corresponds to the situation when the PPPoE protocol packet sniffer and the IPV4 protocol packet sniffer are registered every time that the user logs on the Internet. That is, if the PPPoE server removes the PPPoE protocol packet sniffer from the Linux kernel and the IPV4 protocol packet sniffer from the Netfilter framework, and deletes the user's corresponding information from the authenticated user information, then the PPPoE protocol packet sniffer and the IPV4 protocol packet sniffer need to be registered every time that the user logs on the Internet.

[0069] In the above-described embodiment, the registration and deletion of a IPV4 protocol packet sniffer in the Netfilter framework and a PPPoE protocol packet sniffer in the Linux kernel are used to replace the creation and deletion of a virtual network interface, and the authenticated user information is stored. After receiving the packet, the PPPoE server calls the corresponding protocol packet sniffer and according to the authenticated user information to process the packet header and transmit the processed packet. As such, the correct processing and the normal transmission of the user's uplink data packets and downlink data packets can be ensured. The time cost for the creation of the network interface during the logon process and the time cost for the destruction of the network interface during the logoff process are reduced, such that the logon and logoff speeds for user dial-up during the process of a PPPoE broadband access on the Linux platform can be effectively increased.

[0070] The registration unit 41 is specifically used to register the PPPoE protocol packet sniffer with the Linux kernel and the IPV4 protocol packet sniffer with the POSTROUTING chain of the Netfilter framework.

[0071] The processing unit 43 includes a determination module, a first call module, and a second call module. The determination module is configured to determine whether the packet is a user's uplink packet or a user's downlink packet. The first call modulecommunicated with the determination module is configured, when the packet is the user's uplink packet, to call the PPPoE protocol packet sniffer. The PPPoE protocol packet sniffer determines whether the received packet is a PPPoE data packet and, if the received packet is a PPPoE data packet, according to the authenticated user information, stripsoffheader information of the PPPoE data packet, and forwards the processed PPPoE data packet to the Internet-side. The second call module communicated with the determination module is configured, when the packet is the user's downlink packet, to call the IPV4 protocol packet sniffer. The IPV4 protocol packet sniffer, according to the authenticated user information, adds header information to the user's downlink packet and forwards the processed PPPoE data packet to the user.

[0072] For the user's uplink data packets and downlink data packets, the sniffers used are different and the processing of the header information is also different.

Therefore, the packet needs to be determined to further determine the subsequent processing procedure and realize the normal forwarding of the user's uplink data packets and downlink data packets. At the same time, it is also necessary to determine, according to the authenticated user information stored in advance, whether the current user has authenticated. If the user is not authenticated, the unnecessary packet is directly thrown away to avoid the occupation of resources. If the user is authenticated, the packet is forwarded to the corresponding user or the Internet-side to ensure the smooth transmission of the packet.

[0073] The PPPoE protocol packet sniffer includes: a first determination module configured, according to the value of the Ethernet packet protocol field, to determine that the PPPoE is currently in the PPP Session Stage; a second determination module that is communicated with the first determination module, configured, according to the PPP packet header protocol field, to determine that the packet is a PPPoE data packet; a first acquisition module that is communicated with the second determination module, configured to obtain the MAC address from the Ethernet packet header and the IP address from the IPV4 packet header; a first comparison module that is communicated with the first acquisition module, configured to compare the MAC address and IP address with information in the authenticated user information; a first forwarding module that is communicated with the first comparison module, configured, under the matching situation, to determine that the user belongs to the authenticated users andstrip off header of the PPPoE data packet to forward the processed PPPoE data packet to the Internet-side; a first throw-away module that is communicated with the first comparison module, configured, under the non-matching situation, to determine that the user does not belong to the authenticated users and throw away the PPPoE data packet. If the intercepted packet is not a PPPoE data packet, the processing of the PPPoE control packet is entered, and the control packet processing method will not be discussed in the present disclosure.

[0074] The IPV4 protocol packet sniffer includes: a second acquisition module is configured to obtain the user's IP address from the IPV4 packet header; a second comparison module that is communicated with the second acquisition module, configured to compare the IP address with information in the authenticated user information; a second forwarding module that is communicated with the second comparison module, configured, under the matching situation, to determine that the user belongs to the authenticated users and add the header information to the user's downlink packet to forward the processed packet to the user; a second throw-awaymodule that is communicated with the second comparison module, configured, under the non-matching situation, to determine that the user does not belong to the authenticated users and throw away the downlink packet.

[0075] In practical applications,in the following server configuration,the parallel logon speed increases from 300 per sec to 1000 per sec, and the parallel logoffspeed increases from 200 per sec to 800 per sec. Therefore, the user's logon and logoff speeds can be greatly improved according to the solution of the present disclosure.

Model: PowerEdge R620.
CPU: Intel(R) Xeon(R) CPU E5-2630 v2 @2.60Ght; double.
Random Access Memory (RAM): 64G.
Network card: 82599ES 10-Gigabit SFI/SFP+Network Connection; double
Operating system: CentOS 7.1
Kernel version: Linux-3.10.0-229.1.2.el7

[0076] The foregoing embodiments of the apparatus are merely illustrative, and the units described as separate components may or may not be physically separate, while the components illustrated as units may or may not be physical units, that is, they can be co-located or can be distributed onto a plurality of network elements. A part or all of the modules therein can be selected as required in practice to achieve the objective of the solution of the embodiments. Those ordinarily skilled in the art can appreciate and implement the solution of the embodiments without any inventive effort.

[0077] Through the description of the aforementioned embodiments, a person in the art may clearly understand that the present disclosure may be realized in the form of software plus the necessary common hardware platform. Based on this understanding, the aforementioned technical solution, in essence, or in the form of a contribution to the prior art, or part of thereof, can be embodied in the form of a software product. The computer software product may be stored on a computer-readable media, such as a ROM/RAM, a magnetic disk, or an optical disk, and the like. The computer software product may include a certain number of computer-executable instructions that make a computer device (such as a personal computer, a server, or a network equipment) to execute the methods described in each embodiment, or certain portions of the embodiments, of the present disclosure.

[0078] The foregoing is merely preferred embodiments of the present disclosure and is intended to limit the present disclosure. Any alterations, equivalents, or advantages within the spirit and principles of the present disclosure are intended to be encompassed within the scope of the present invention.

Claims

1. A method for transmittingPoint-to-Point Protocol over Ethernet (PPPoE) packets, comprising:

registering, bya PPPoE server, a PPPoE protocol packet sniffer with a Linux kernel and an In-

ternet Protocol Version 4 (IPV4) protocol packet sniffer with a Netfilter framework, and adding a user's Internet Protocol (IP) address and media access control (MAC) address to authenticated user information;
receiving, bythe PPPoE server, a packet; and
calling, bythe PPPoE server, the PPPoE protocol packet sniffer or the IPV4 protocol packet sniffer to process and transmit the packet according to the authenticated user information.

2. The method according to claim 1, wherein calling, bythe PPPoE server, the PPPoE protocol packet sniffer or the IPV4 protocol packet sniffer to process and transmit the packet according to the authenticated user information, includes:

determining, by the PPPoE server, whether the packet is a user's uplink packet or a user's downlink packet;
when the packet is the user's uplink packet, calling, bythe PPPoE server, the PPPoE protocol packet sniffer, and determining, by the PPPoE protocol packet sniffer, whether the packet is a PPPoE data packet and, when the packet is the PPPoE data packet, according to the authenticated user information, striping off header information of the PPPoE data packet, and forwarding the processed PPPoE data packet to the Internet-side; and
when the packet is the user's downlink packet, calling, by the PPPoE server, the IPV4 protocol packet sniffer, and adding, by the IPV4 protocol packet sniffer, according to the authenticated user information, header information to the user's downlink packet and forwarding the processed PPPoE data packet to the user.

3. The method according to claim 2, whereincalling, bythe PPPoE server, the PPPoE protocol packet sniffer, and determining, bythe PPPoE protocol packet sniffer,whether the packet is the PPPoE data packet and, when the packet is the PPPoE data packet, according to the authenticated user information, striping off the header information of the PPPoE data packet, and forwarding the processed PPPoE data packet to the Internet-side, includes:

determining, by the PPPoE protocol packet sniffer, according to a value of an Ethernet packet protocol field, that the PPPoE is currently in aPPP Session Stage;
determining, by the PPPoE protocol packet sniffer, according to a PPP packet header protocol field, that the packet is the PPPoE data packet;
obtaining, by the PPPoE protocol packet sniffer, the MAC address from an Ethernet packet header and the IP address from an IPV4 packet header;
comparing, by the PPPoE protocol packet sniffer, the MAC address and IP address with information in the authenticated user information;
when the MAC address and IP addressmatch with information in the authenticated user information, determining that the user belongs to authenticated users and striping off the header of the PPPoE data packet to forward the processed PPPoE data packet to the Internet-side; and
when the MAC address and IP address do not match with information in the authenticated user information, determining that the user does not belong to the authenticated users and throwing away the PPPoE data packet.

4. The method according to claim 2, whereincalling, bythe PPPoE server,the IPV4 protocol packet sniffer, and adding, bythe IPV4 protocol packet sniffer, according to the authenticated user information, header information to the user's downlink packet and forwarding the processed PPPoE data packet to the user, includes:

obtaining, by the IPV4 protocol packet sniffer, the user's IP address from the IPV4 packet header;
comparing, by the IPV4 protocol packet sniffer, the IP address with the information in the authenticated user information;
when the IP address matches with the information in the authenticated user information, determining that the user belongs to the authenticated users and adds the header information to the user's downlink packet to forward the processed packet to the user; and
when the IP address does not match with the information in the authenticated user information, determining that the user does not belong to the authenticated users and throwing away the downlink packet.

5. The method according to any one of claims 1-4, further including:

Registering, by the PPPoE server,the PPPoE protocol packet sniffer with the Linux kernel and the IPV4 protocol packet sniffer with the Netfilter framework every time the user logs on successfully; and
every time after the user successfully logs off, removing, by the PPPoE server,the PPPoE protocol packet sniffer from the Linux kernel and the IPV4 protocol packet sniffer from the Netfilter framework, and deleting corresponding information of the user who successfully logs off from

the authenticated user information.

6. The method according to any one of claims 1-4, further including:

when the user logs on the Internet for a first time after user initializing or restarting,registering the PPPoE protocol packet sniffer with the Linux kernel and the IPV4 protocol packet sniffer with the Netfilter framework; and
after the user successfully logs off, deleting the user's corresponding information from the authenticated user information

7. The method according to any one of claims 1-4, further including:
registering, bythe PPPoE server, the IPV4 protocol packet sniffer with a POSTROUTING chain of the Netfilter framework.

8. An Point-to-Point Protocol over Ethernet (PPPoE)server,comprising:

a registration unit configured to register a PPPoE protocol packet sniffer with a Linux kernel and an IPV4 protocol packet sniffer with aNetfilter framework, and add a user's IP address and MAC address to authenticated user information;
a receiving unit configured to receive a packet; and
a processing unit configured to call the PPPoE protocol packet sniffer or the IPV4 protocol packet sniffer and, according to the authenticated user information, process and transmit the packet.

9. The PPPoEserver according to claim 8, wherein the processing unit includes:

a determination module configured to determine whether the packet is a user's uplink packet or a user's downlink packet;
a first call module configured, when the packet is the user's uplink packet, to call the PPPoE protocol packet sniffer, the PPPoE protocol packet sniffer determines whether the packet is a PPPoE data packet and, when the received packet is the PPPoE data packet, according to the authenticated user information, strips off-header information of the PPPoE data packet, and forwards the processed PPPoE data packet to the Internet-side; and
a second call module configured, when the packet is the user's downlink packet, to call the IPV4 protocol packet sniffer, the IPV4 protocol packet sniffer, according to the authenticated user information, adds header information to the user's downlink packet and forwards the processed PPPoE data packet to the user.

10. The PPPoE server according to claim 9, wherein the PPPoE protocol packet sniffer includes:

a first determination module configured, according to a value of an Ethernet packet protocol field, to determine that the PPPoE is currently in aPPP Session Stage;
a second determination module configured, according to a PPP packet header protocol field, to determine that the packet is the PPPoE data packet;
a first acquisition module configured to obtain the MAC address from an Ethernet packet header and the IP address from an IPV4 packet header;
a first comparison module configured to compare the MAC address and IP address with information in the authenticated user information;
a first forwarding module configured, when the MAC address and IP address match with information in the authenticated user information, to determine that the user belongs to authenticated users andstrip off header of the PPPoE data packet to forward the processed PPPoE data packet to the Internet-side; and
a first throw-away module configured, when the MAC address and IP address do not match with information in the authenticated user information, to determine that the user does not belong to the authenticated users and throw away the PPPoE data packet.

11. The PPPoE server according to claim 9, wherein the IPV4 protocol packet sniffer includes:

a second acquisition module configured to obtain the user's IP address from the IPV4 packet header;
a second comparison module configured to compare the IP address with the information in the authenticated user information;
a second forwarding module configured, when the IP address matches with information in the authenticated user information, to determine that the user belongs to the authenticated users and add the header information to the user's downlink packet to forward the processed packet to the user; and
a second throw-away module configured, when the IP address does not match with information in the authenticated user information, to determine that the user does not belong to the authenticated users and throw away the downlink packet.

12. The PPPoE server according to any one of claim

8-11, further including:
a removing unit configured, after the user successfully logs off, to remove the PPPoE protocol packet sniffer from the Linux kernel and the IPV4 protocol packet sniffer from the Netfilter framework, and to delete the user's corresponding information from the authenticated user information.

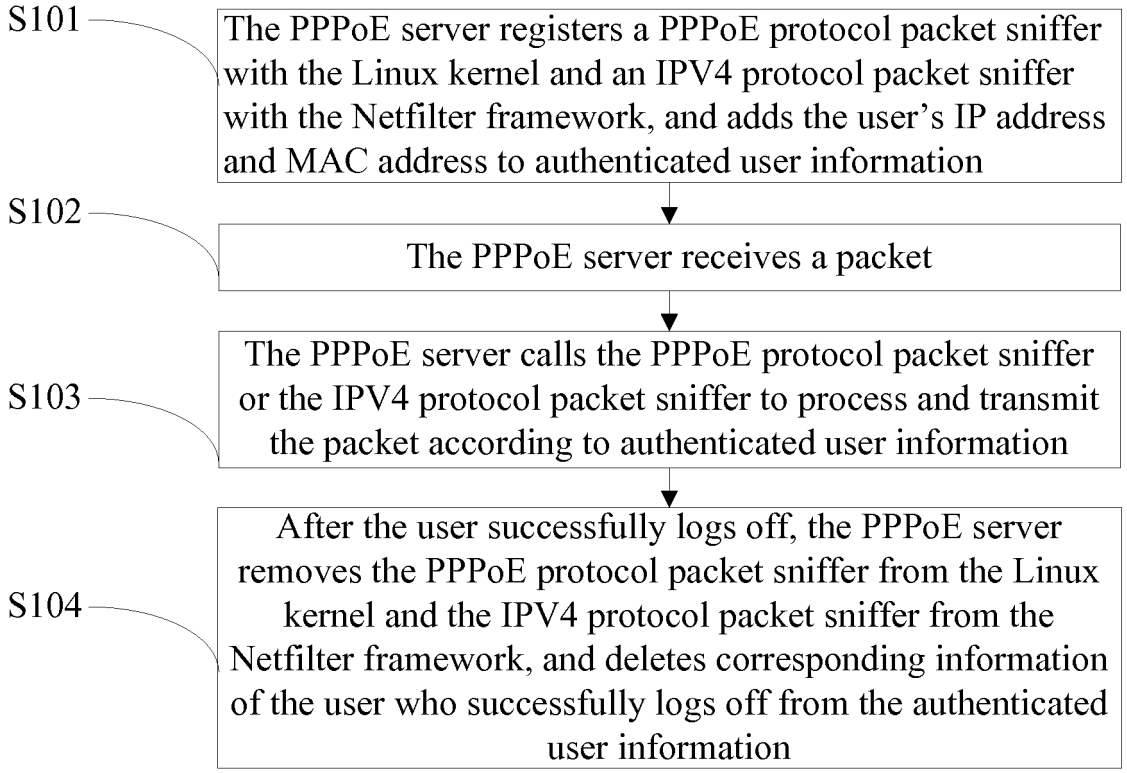
S101
The PPPoE server registers a PPPoE protocol packet sniffer with the Linux kernel and an IPV4 protocol packet sniffer with the Netfilter framework, and adds the user's IP address and MAC address to authenticated user information
S102
The PPPoE server receives a packet
S103
The PPPoE server calls the PPPoE protocol packet sniffer or the IPV4 protocol packet sniffer to process and transmit the packet according to authenticated user information
S104
After the user successfully logs off, the PPPoE server removes the PPPoE protocol packet sniffer from the Linux kernel and the IPV4 protocol packet sniffer from the Netfilter framework, and deletes corresponding information of the user who successfully logs off from the authenticated user information

FIG. 1

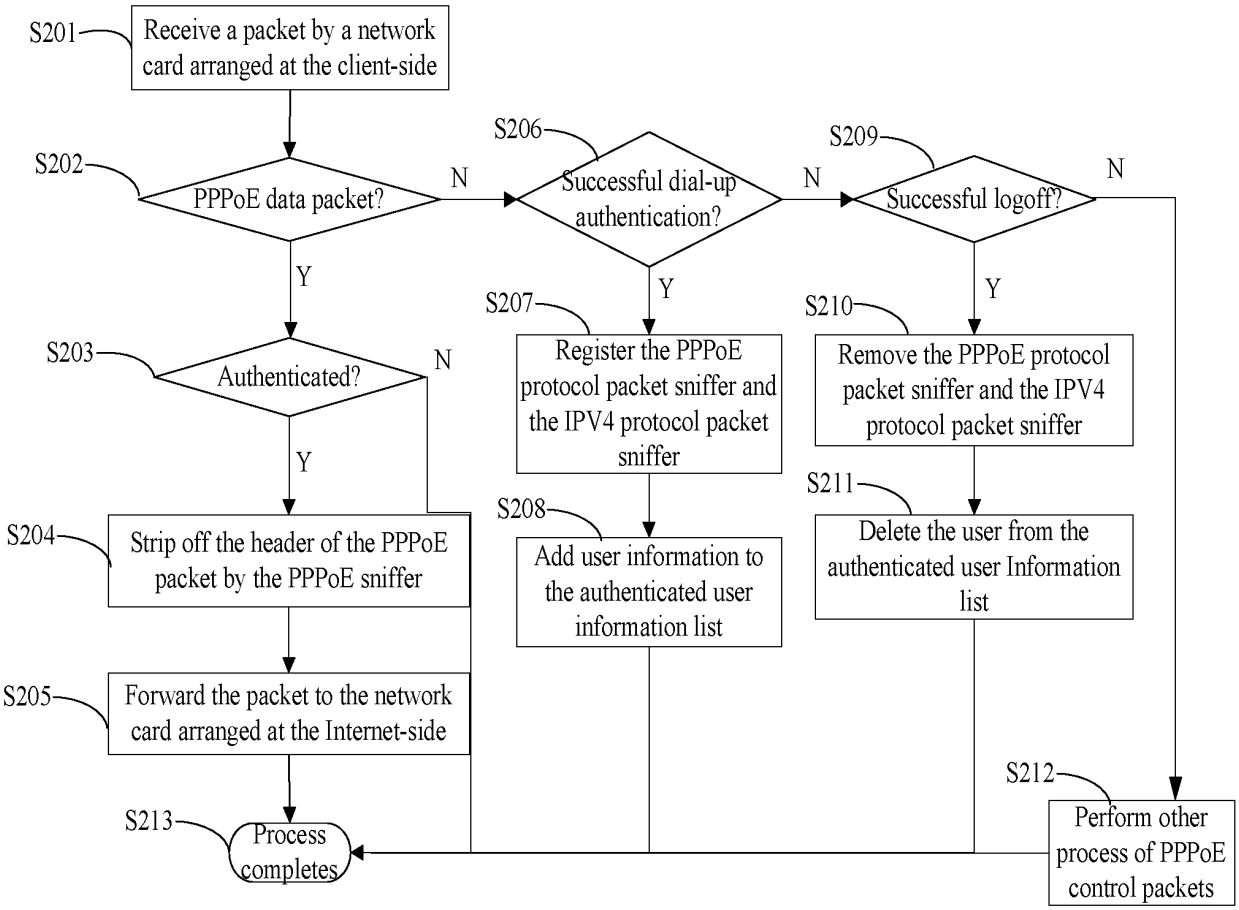
S201
Receive a packet by a network card arranged at the client-side
S202
PPPoE data packet?
N
Y
S203
Authenticated?
N
Y
S204
Strip off the header of the PPPoE packet by the PPPoE sniffer
S205
Forward the packet to the network card arranged at the Internet-side
S213
Process completes
S206
Successful dial-up authentication?
N
Y
S207
Register the PPPoE protocol packet sniffer and the IPV4 protocol packet sniffer
S208
Add user information to the authenticated user information list
S209
Successful logoff?
N
Y
S210
Remove the PPPoE protocol packet sniffer and the IPV4 protocol packet sniffer
S211
Delete the user from the authenticated user Information list
S212
Perform other process of PPPoE control packets

FIG. 2

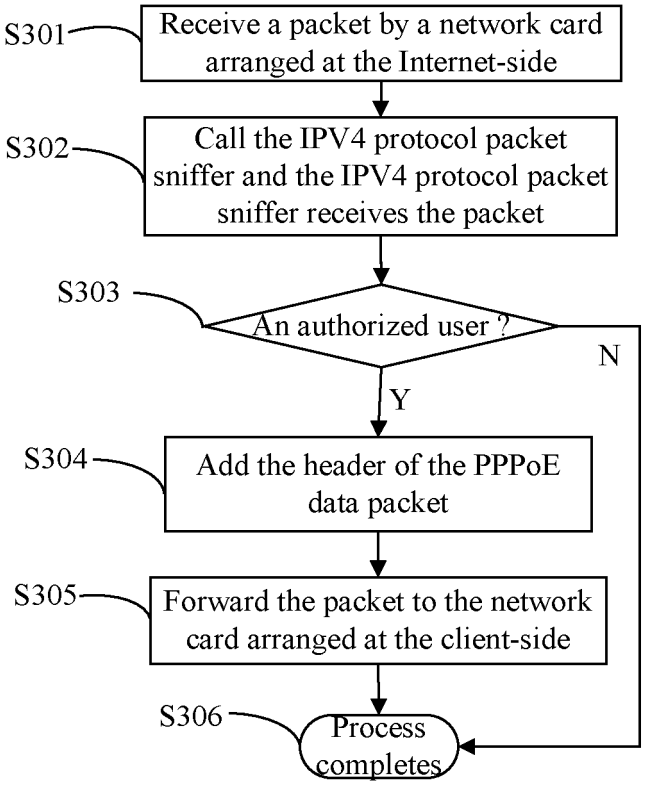
S301
Receive a packet by a network card arranged at the Internet-side
S302
Call the IPV4 protocol packet sniffer and the IPV4 protocol packet sniffer receives the packet
S303
An authorized user ?
N
Y
S304
Add the header of the PPPoE data packet
S305
Forward the packet to the network card arranged at the client-side
S306
Process completes

FIG. 3

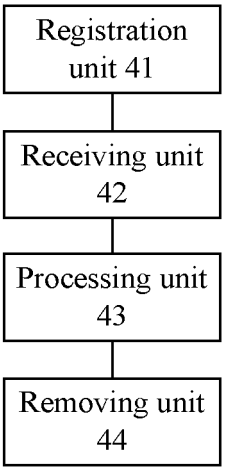
Registration unit 41
Receiving unit 42
Processing unit 43
Removing unit 44

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/080245

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/741 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC, GOOGLE: PPPoE, 以太网, 点对点, 点到点, 报文, 包, 帧, 拦截, 过滤, 捕, 抓, MAC, 媒体访问控制, 媒体接入控制, 介质访问控制, 介质接入控制, 媒介访问控制, 媒介接入控制, IP, IPv4, 因特网协议, 英特网协议, 互联网协议, 认证, 授权, point to point over ethernet, packet, frame, netfilter, filter, capture, internet protocol, media access control, medium access control, valid+, auth+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101079887 A (HITACHI COMMUNICATION TECHNOLOGIES LTD.), 28 November 2007 (28.11.2007), description, page 7, paragraph 1 to page 19, paragraph 2, and figures 1-21	1-12
A	CN 102664833 A (FIBERHOME TELECOMMUNICATION TECHNOLOGIES CO., LTD.), 12 September 2012 (12.09.2012), entire document	1-12
A	CN 1790987 A (SAMSUNG SDI CO., LTD.), 21 June 2006 (21.06.2006), entire document	1-12
A	CN 104243454 A (H3C TECHNOLOGIES CO., LIMITED), 24 December 2014 (24.12.2014), entire document	1-12
A	US 2011161510 A1 (ARRIS GROUP INC.), 30 June 2011 (30.06.2011), entire document	1-12

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 November 2017	04 January 2018

Name and mailing address of the ISA	Authorized officer
State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	LI, Wen Telephone No. (86-10) 62413333

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/080245

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101079887 A	28 November 2007	JP 2007312289 A	29 November 2007
		US 2007274290 A1	29 November 2007
CN 102664833 A	12 September 2012	WO 2013163852 A1	07 November 2013
		RU 2013155980 A	27 June 2015
		SG 2014015259 A	28 March 2014
CN 1790987 A	21 June 2006	US 2006137005 A1	22 June 2006
		KR 20060068211 A	21 June 2006
		JP 2006178976 A	06 July 2006
CN 104243454 A	24 December 2014	None	
US 2011161510 A1	30 June 2011	None	

Form PCT/ISA/210 (patent family annex) (July 2009)